

## UNITED STATES DISTRICT COURT

for the  
Eastern District of VirginiaIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)7 W Sedgwick Street  
Sandston, VA 23150

Case No. 3:17sw151

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, fully incorporated by reference herein;

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, fully incorporated by reference herein.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| Code Section      | Offense Description                                       |
|-------------------|-----------------------------------------------------------|
| 18 U.S.C. § 2251  | Production of Child Pornography                           |
| 18 U.S.C. § 2252A | Possession, Receipt and Distribution of Child Pornography |

The application is based on these facts:

See attached Affidavit, fully incorporated by reference herein.

- ☐ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

John Houlberg, FBI Task Force Officer

Printed name and title

Sworn to before me and signed in my presence.

Date:

July 19, 2017

ISI

David J. Novak  
United States Magistrate Judge

Judge's signature

City and state: Richmond, Virginia

United States Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Richmond Division

IN THE MATTER OF THE SEARCH OF:  
The premises known as  
7 W Sedgwick Street  
Sandston, VA 23150

Case No. 3:17SW151

**FILED UNDER SEAL**

**AFFIDAVIT IN SUPPORT OF AN  
APPLICATION UNDER RULE 41 FOR A  
WARRANT TO SEARCH AND SEIZE**

I, John P. Houlberg, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 7 W Sedgwick Street, Sandston, VA 23150, hereinafter "SUBJECT PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Virginia State Police Bureau of Criminal Investigation, General Investigations Section, and have been since 1999. I am currently assigned as a Task Force Officer (TFO) to the Federal Bureau of Investigation, Richmond Division Child Exploitation Task Force and have been since 2011. I have participated in investigations involving sexual assaults, pedophiles, preferential child molesters, persons who produce, collect, and distribute child pornography, and the importation and distribution of materials relating to the sexual exploitation of children. I have received training from the FBI in the areas of sexual

assaults and child exploitation, and I have reviewed images and videos of child pornography in a wide variety of media forms, including computer media. I have also discussed and reviewed these materials with other law enforcement officers.

3. In the course of my employment as a sworn law enforcement officer, I have participated in the execution of numerous search warrants resulting in the seizure of computers, magnetic storage media for computers, other electronic media, and other items evidencing violations of state and federal laws, including various sections of Title 18, United States Code, Sections 2251, 2252 and 2252A involving child exploitation offenses.

4. I have been deputized as a Special Deputy United States Marshal since May 20, 2011. As a Special Deputy United States Marshal, your Affiant is authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

5. The statements in this affidavit are based in part on my investigation of this matter and on information provided by other law enforcement agents. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence, contraband, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252 and 2252A, are presently located at the SUBJECT PREMISES.

6. The purpose of the application which this affidavit supports is to obtain court authorization to seize evidence, more particularly described in Attachment B, of violations of 18 U.S.C. § 2251, which make it a crime to produce child pornography, 18 U.S.C. §§ 2252(a)(4)(B)

and 2252A(a)(5)(B), which make it a crime to possess or access with intent to view child pornography, and 18 U.S.C. §§ 2252(a)(2) and 2252A(a)(2), which make it a crime to receive and distribute child pornography. I am requesting authority to search the entire premises, including the residential dwelling and any computer and computer media located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as contraband, instrumentalities, and evidence of a crime.

7. In summary, the following affidavit sets forth facts that establish that there is probable cause to believe a subject using the IP address 98.117.73.10 and Kik username Strigoi33 produced child pornography, and received and/or transmitted, via the Internet, images depicting minors engaging in sexually explicit activity, and that there is probable cause to believe the person associated with IP address 98.117.73.10 and Kik username Strigoi33 is in possession of and received and transmitted the aforementioned material using a computer or electronic device that is presently located at the SUBJECT PREMISES.

#### **RELEVANT STATUTORY PROVISIONS**

8. **Distribution or Receipt of Child Pornography:** 18 U.S.C. § 2252A(a)(2) provides that it is a crime to knowingly receive or distribute any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

9. **Child pornography** means any visual depiction, in any format, of sexually explicit conduct where: (A) the production involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital or computer-generated image that is substantially indistinguishable from that of a minor engaged in sexually explicit conduct; or (C)

such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexual explicit conduct. *See* 18 U.S.C. § 2256(8).

10. **Visual depictions** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which are capable of conversion into a visual image, and data which are capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. *See* 18 U.S.C. § 2256(5).

11. **Minor** means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

12. **Sexually explicit conduct** means actual or simulated: (i) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person. *See* 18 U.S.C. § 2256(2).

### **DEFINITIONS**

13. The **Internet** is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

14. **Internet Protocol address (or simply “IP address”)** is a unique numeric address used by computers on the Internet. A typical IP address looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 121.56.97.178). Newer IP addresses use a IPv6 format, represented as eight groups of four hexadecimal digits with the groups being separated by colons, for example 2001:0db8:0000:0042:0000:8a2e:0370:7334. Every computer attached

to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

15. **Storage medium** is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

16. **Log Files** are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

17. **Internet Service Providers or ISPs** are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone-based dial-up, broadband-based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user

name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

18. **Kik Messenger** is a free instant messaging application for mobile devices from Kik Interactive, available on iOS, Android, and Windows Phone operating systems.

19. **Dropbox** is a file hosting service that offers cloud storage, file synchronization across multiple devices and file sharing between individuals. Dropbox offers users two gigabytes of free storage and several fee-based plans with a variety of features and either two terabytes or an unlimited quantity of storage (depending on the plan). Dropbox users can share files with others by creating a shared folder within their account and sending a hyperlink (“link”) to the other user, who can then access the shared folder and download the files.

20. **Smartphone** is a portable personal computer with a mobile operating system having features useful for mobile or handheld use. Smartphones, which are typically pocket-sized (as opposed to tablets, which are larger in measurement), have become commonplace in modern society in developed nations. While the functionality of smartphones may vary somewhat from model to model, they typically possess most if not all of the following features and capabilities: 1) place and receive voice and video calls; 2) create, send and receive text messages; 3) voice-activated digital assistants (such as Siri, Google Assistant, Alexa, Cortana, or Bixby) designed to enhance the user experience; 4) event calendars; 5) contact lists; 6) media players; 7) video games; 8) GPS navigation; 9) digital camera and digital video camera; and 10) third-part software components commonly referred to as “apps.” Smartphones can access

the Internet through cellular as well as Wi-Fi (“wireless fidelity”) networks. They typically have a color display with a graphical user interface that covers most of the front surface of the phone and which usually functions as a touchscreen and sometimes additionally as a touch-enabled keyboard.

21. **SIM card** stands for a “subscriber identity module” or “subscriber identification module,” which is the name for an integrated circuit used in mobile phones that is designed to securely store the phone’s international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers). It is also possible to store contact information on many SIM cards.

22. The terms “**records**,” “**documents**,” and “**materials**,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Smartphones, Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).



**CHARACTERISTICS OF COLLECTORS OF CHILD PORNOGRAPHY**

23. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter “collectors”).

24. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.

25. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature and sexual aids.

26. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.

27. Collectors almost always possess and maintain their “hard copies” of child pornographic images and reference materials (*e.g.*, mailing and address lists) in a private and

secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically these materials are kept at the collector's residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods, even for years. Collectors often discard child pornography images only while "culling" their collections to improve their overall quality.

28. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.

29. Collectors prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

30. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during nationwide law enforcement initiatives.

#### **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

31. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is digital data stored on a computer's hard drive or

other storage media, or on a smartphone's internal memory or SIM card. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

32. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Depending on a variety of factors, a particular computer could easily not overwrite deleted files with new data for many months, and in certain cases conceivably ever.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

33. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers,

e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.
- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an

accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to possess, receive, distribute and/or produce child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the

offense.

34. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and

configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

35. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

36. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.



**SPECIFICITY OF SEARCH WARRANT RETURN AND NOTICE REGARDING  
INITIATION OF FORENSIC EXAMINATION**

37. Consistent with the Court's current policy, the search warrant return will list the model(s) and serial number(s) of any and all computers seized at the SUBJECT PREMISES, and include a general description of any and all associated peripheral equipment that has been seized. Additionally, the search warrant return will include the total numbers of each type of digital media that has been seized (*e.g.*, "ten (10) 3.5" diskettes; twenty (20) CDs; twenty (20) DVDs; three (3) USB drives; one (1) 256 MB flash memory card," *etc.*)

38. Moreover, the Government will file a written pleading in this case within one hundred twenty (120) days after the execution of the search warrant notifying the court that the imaging process of digital evidence seized from the target location is complete, and the forensic analysis of computers and media has begun. Such notice will include confirmation that written notice has been provided to the defendant or his counsel informing the defendant that the forensic examination of evidence seized from him has actually begun. Such notice to the defendant and the Court is not intended to mean, and should not be construed to mean, that the forensic analysis is complete, or that a written report detailing the results of the examination to date will be filed with the Court or provided to the defendant or his counsel. This notice does not create, and is not meant to create, additional discovery rights for the defendant. Rather, the sole purpose of this notice is to notify the defendant that, beyond the simple seizure of his property, a forensic search of that property has actually begun.

**PROBABLE CAUSE**

39. I received information from a task force officer (TFO) assigned to the FBI's Washington Field Office (WFO) who was acting in an undercover capacity (UC) as part of the

Metropolitan Police Department-Federal Bureau of Investigation (“MPD-FBI”) Child Exploitation Task Force. In that capacity, the UC navigated to an online website that law enforcement officials know is frequented by individuals who have a sexual interest in children and incest, among other fetishes. There he posted an advertisement that was meant to attract individuals with a sexual interest in children, which read, “Looking to meet other taboo Dads/moms for chat n more, don't want to say to much on here but shoot me an email with your KIK if interested”.

40. On Monday June 26, 2017, an individual (not fully identified) responded to the UC's advertisement via email stating, “Daddy” here. Kik Strigoi33. Very interested”. The UC began communicating with this individual via Kik Messenger. This individual was using the Kik name, “strigoi33” with a display name of, “La Sorciere.” “strigoi33” identified himself as a 36-year-old male residing in Richmond, Virginia. During the course of the chat “strigoi33” stated that he was into taboo but did not have any children. The UC informed “strigoi33” that he had a 9-year-old daughter. “strigoi33” responded, “Have you started 'teaching' her, or is that not your thing? I mean no offense. Just curious.” “strigoi33” later stated, “Lucky. I'd love to teach a yung girl to suck. Youngest I've played with was 14.”

41. The UC asked “strigoi33” about the 14 year-old girl. “strigoi33” stated, “She's a girl I met online. Mixed black and white.” “strigoi33” sent the UC a link to a Dropbox folder containing six videos. I have reviewed the videos, and based on my training and experience believe that four of them depict child pornography as defined in 18 U.S.C. § 2256(8). The four files are described below:

- a. A video of a minor female being vaginally penetrated by an adult male penis. The child is naked and lying on her back with her legs spread. The adult male is standing over her in between her legs. It appears the adult male's penis will not fully penetrate the child's vagina and she can be heard gasping in what sounds like pain. The child appears to be between 12-14 years old.
- b. A video of a prepubescent female naked and lying on her back with her legs spread. The child lifts her legs up overhead showing her vagina. An adult male is standing over her attempting to force his erect penis in her vagina. He is talking to her in what appears to be another language. The minor appears to be between 10-12 years old.
- c. A video depicting an adult woman and a prepubescent male, approximately 6-8 years old. They are both nude and the boy is standing in front of the female, in what appears to be a bathroom. The adult female is performing oral sex on the boy.
- d. A video of a prepubescent male, approximately 8-10 years old, nude and lying on his back on a blanket. An adult woman is clothed and sitting facing towards him in between his legs. The adult female is masturbating the boy's penis and kissing his penis. They are speaking to each other in an unidentified language.

42. During the course of the chat "strigoi33" stated, "You're so lucky. Though I have to admit, I'd be scared to play with my own daughter. I was worried the 14yo was going to be a cop." "strigoi33" sent the UC a video that he claimed was the 14 year-old girl. I reviewed the video, which depicts an adult black male standing in front of a female who is on her knees facing

him. The female appears to be naked from the waist down and is wearing a dark colored t-shirt with white and green letters on it. The male is masturbating his penis while rubbing it on her face and ejaculates on her face. The female appears to be between 13-15 years old. The male is heard on the video saying, "Oh shit, lick the tip." The child then licks what appears to be semen from the end of his penis and he says to her, "good girl". She then smiles for the camera. The male has a large silver tone ring on his left index finger.

43. The UC asked "strigoi33," "How young would u go". "strigoi33" responded, "Fucking, about 13-12. Oral around your daughter's age maybe 7. As long as they are enjoying it and eager to learn. I wouldn't want to hurt or force anyone. Not my thing."

44. During the course of the chat "strigoi33" sent another video of that girl that he claims to have had sexual contact with. I reviewed the video, which depicts what appears to be the same female from the previous one and she is wearing the same t-shirt. The female is kneeling facing towards the camera and performing oral sex on an erect black male's penis. The male says, "You like being filmed don't you?" The child is then heard saying, "Mm hmm." The male responds, "That's a good girl" and pulls his t-shirt up exposing more of his penis for the video. It appears he has on the same silver tone ring on his left index finger from the previous video. The male can be heard saying I will send you this video but you cannot show it to anyone.

45. An emergency disclosure request was sent to Kik for subscriber information associated with the target username. Kik's response provided an unconfirmed email address of [la\\_sorciere33@yahoo.com](mailto:la_sorciere33@yahoo.com) and IP logs between May 29, 2017, and June 28, 2017. Examination of the logs provided by Kik revealed the primary way in which this account was accessed was

via T-Mobile wireless internet access. Those logs further revealed that in addition to T-Mobile IP addresses the Kik account was accessed via the same Verizon FiOS IP address (98.117.73.10) between June 9 and 25, 2017. An emergency request was sent to Verizon for subscriber information associated with this single IP address. Verizon called WFO and identified the subscriber as Tammie Ellis, 7 W Sedgwick Street, Sandston VA 23150, email address [tj\\_ellis83@yahoo.com](mailto:tj_ellis83@yahoo.com).

46. Searches of public records indicate that Tammie Ellis resides in Henrico County, at the SUBJECT PREMISES. Additional residents at the SUBJECT PREMISES are Charles Ellis, who appears to be the husband of Tammie Ellis; and Eric Ellis, who appears to be the brother of Charles Ellis. Photographs available during public record searches depict Charles Ellis with a large silver ring on his left index finger, consistent with the ring observed during the videos received by the UC.

47. A search of the Virginia Department of Motor Vehicles database indicates that Tammie Ellis, Charles Ellis, and Eric Ellis list an address of the SUBJECT PREMISES.

48. On July 7, 2017, I conducted a spot surveillance of the SUBJECT PREMISES. I observed that the residence is a single-story house with white siding and green shutters. The front entry door sits in the front center of the house, with a concrete porch leading up to the door. In front of the porch is a small wooden ramp leading to a sidewalk that leads to the edge of the street. There is a covered roof over the front porch with the number "7" in black on one of the pillars to the left of the entry door. There is a driveway on the left side of the property leading to what appears to be a carport in the back yard. In between the driveway and the front sidewalk is a small wooden fence by the edge of the road. I observed a blue in color Dodge minivan with

Virginia License # VNN-6758 in the driveway. Virginia Department of Motor Vehicle records showed the vehicle registered to Charles Tiffit Ellis Jr, social security account number XXX-XX-5503, date of birth XX/XX/1980, and showing an address of 7 W Sedgwick St, Sandston, VA 23150.

### **CONCLUSION**


49. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that (1) an individual or individuals at the SUBJECT PREMISES used a computer or electronic device connected to the Internet from the SUBJECT PREMISES to violate Title 18, United States Code §§ 2251, 2252 and 2252A, and (2) the fruits, evidence, contraband and instrumentalities of these offenses, described in Attachment B, are presently located at the SUBJECT PREMISES. Permission is expressly sought to seize any computer hardware, computer software, and computer related documentation located at the SUBJECT PREMISES and subsequently conduct an on-site and off-site forensic examination, as necessary, using whatever data analysis techniques are needed to seize the contraband, evidence, and instrumentalities listed in Attachment B.

50. I respectfully request, therefore, that the Court issue the attached warrant authorizing the search and seizure of the items listed in Attachment B.

---

John P. Houlberg  
Special Deputy United States Marshal  
FBI Child Exploitation Task Force  
Federal Bureau of Investigation

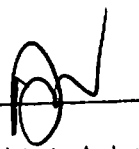
SEEN AND APPROVED BY:



---

Janet Lin Ah Lee  
Assistant United States Attorney

SUBSCRIBED and SWORN  
before me on July 19, 2017



IS/  
David J. Novak  
United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Richmond Division

IN THE MATTER OF THE SEARCH OF:

The premises known as  
7 W Sedgwick Street  
Sandston, VA 23150

Case No. \_\_\_\_\_

**FILED UNDER SEAL**

**ATTACHMENT A**

**DESCRIPTION OF PREMISES TO BE SEARCHED**

The premises to be searched is known as 7 W Sedgwick Street, Sandston, VA 23150. The premises is described as a single story house with white siding and green shutters. The front entry door sits in the front center of the house, with a concrete porch leading up to the door. In front of the porch is a small wooden ramp leading to a sidewalk that leads to the edge of the street. There is a covered roof over the front porch with the number "7" in black on one of the pillars to the left of the entry door. There is a driveway on the left side of the property leading to what appears to be a carport in the back yard. In between the driveway and the front sidewalk is a small wooden fence by the edge of the road. The area to be searched includes all rooms and other parts therein and any storage rooms, storage areas, or any other outbuildings of any kind associated with the premises.



IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Richmond Division

IN THE MATTER OF THE SEARCH OF:

The premises known as  
7 W Sedgwick Street  
Sandston, VA 23150

Case No. \_\_\_\_\_

**FILED UNDER SEAL**

**ATTACHMENT B**

*Property to be seized*

1. All records relating to violations of 18 U.S.C. §§ 2251, 2252 and 2252A relating to the production, distribution, receipt and possession of child pornography, including:

- a. Any and all visual depictions of minors;
- b. Any and all address books, names, and lists of names and addresses of minors;
- c. Any and all diaries, notebooks, notes, and any other records reflecting physical contact, whether real or imagined, with minors, and any such items discussing sexual activities with minors;
- d. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids;
- e. Records and information relating to the e-mail accounts  
la\_sorciere33@yahoo.com and tj\_ellis83@yahoo.com and any related email accounts;

- f. Records and information relating to Kik username/account “strigoi33” and any related Kik accounts;
  - g. Records and information relating to the location, past or present, of Charles Ellis;
  - h. Records and information relating to communications with Internet Protocol addresses 98.117.73.10.
- 2. Computers or storage media used as a means to commit the violations described above.
- 3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):
  - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
  - c. evidence of the lack of such malicious software;

- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
  - e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
  - f. evidence of the times the COMPUTER was used;
  - g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
  - h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
  - i. records of or information about Internet Protocol addresses used by the COMPUTER;
  - j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
  - k. contextual information necessary to understand the evidence described in this attachment.
4. Routers, modems, and network equipment used to connect computers to the Internet.

5. Silver-colored ring as described in the Affidavit and as depicted in the photograph included in this Attachment.

6. During the course of the search, law enforcement officials may photograph the searched SUBJECT PREMISES to record the condition thereof and/or the location of items therein.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

